

кабинета получает доступ к серверу, на котором хранятся данные, выгруженные с мобильного телефона жертвы. Стоит отметить, что такие приложения работают незаметно для владельца смартфона, явно не обнаруживаются в файловой системе и в запущенных процессах телефона. Признаком внедрения такого приложения может быть увеличение объема принимаемых и отсылаемых данных посредством сети Интернет или постоянно разряжающийся аккумулятор смартфона.

К популярным программам слежения относятся: FlexiSPY Extreme, Pro-X и Full от компании MobControl. Найти их в свободном обращении в сети Интернет практически невозможно, как и другие программы слежения.

Таким образом, получить и перехватить данные с мобильного устройства можно с помощью специально внедренных аппаратных закладок, без использования сложных технических средств физического перехвата сотовой связи. Для того чтобы защититься от внедрения программных средств перехвата сотовой связи, достаточно придерживаться следующих правил:

- обеспечить противодействие несанкционированному доступу к мобильному устройству;
- предусмотреть меры по защите смартфона от внедрения вредоносных приложений.

Для предотвращения перехвата информации с помощью аппаратных средств можно использовать приложения, которые позволяют выявить ложные базовые станции и отследить любую подозрительную активности в сети, в том числе при использовании SMS.

УДК 004.056.53

И. Ю. Петров

Научный руководитель: д-р тех. наук, проф. С. В. Поршнева
Уральский федеральный университет, Екатеринбург

ОБНАРУЖЕНИЕ ПЭМИ С ПОМОЩЬЮ RTL-SDR-ПРИЕМНИКА

Аннотация. Проведен анализ возможностей ТВ-тюнера на чипе RTL2832U по захвату и оцифровке радиосигнала с целью его использования в составе программно-определяемой радиосистемы.

Ключевые слова: информационная безопасность; побочные электромагнитные излучения; программно-определяемая радиосистема; радиомониторинг эфира.

Сегодня уже невозможно представить себе нашу жизнь без современных электронных средств обработки, хранения и передачи информации. Широкие возможности и качество, которые предоставляют цифровые электронные средства, предопределили их массовое распространение. Однако уже в конце 70-х годов в открытой печати появились публикации о возможном радиотехническом канале утечки информации, обрабатываемой с помощью средств цифровой техники. Особую актуальность эта тема приобрела в настоящее время. Побочные электромагнитные излучения — вид электромагнитных волн, возникающих в результате работы электрических приборов, в частности протекания электрического тока по проводникам. Так как электромагнитные излучения есть возмущения электромагнитного поля, то при передаче информации через коммутирующие соединения с помощью кабелей возникают электромагнитные излучения, которые при попадании на проводник (антенну считывающего устройства), порождают в нем ток, схожий с оригиналом. После дискретизации считанного сигнала можно восстановить данные передаваемые через проводник, что может привести к утечки конфиденциальной информации.

В настоящее время для проведения исследований ПЭМИ технических средств целесообразно использовать такой комплекс аппаратуры, основу которого составляет измерительный приемник или анализатор спектра с набором соответствующих измерительных антенн. Измерительные приемники в наибольшей степени отвечают требованиям, предъявляемым к аппаратуре для исследований ПЭМИ. Они обеспечивают высокую точность измерений. Значительная часть измерительных приемников позволяет наблюдать панораму исследуемого диапазона частот, анализировать сигналы на выходе детекторов различных типов. Однако цена измерительных приемников весьма высока. В связи с этим возникает задача создания таких условий, при которых будет возможно проводить научную деятельность по освоению канала утечки информации ПЭМИ с минимизацией затрат на приобретение оборудования.

Одним из ключевых вопросов обнаружения ПЭМИ является радиомониторинг эфира. На данный момент на рынке представлено достаточное количество комплексов радиомониторинга, позволяющих успешно решать данную задачу, но не подходящих для исследовательских целей ввиду высокой стоимости и сложности приобретения [1].

Адекватным решением в данном сегменте является построение приемника сигналов с возможностями сканирования широкого диапазона частот, анализа и демодуляции обнаруженных радиосигналов по технологии SDR с использованием обычного компьютера для реализации программной компоненты. Доступным вариантом аппаратной компоненты программно-определяемой радиосистемы, реализующей функции захвата и оцифровки радиосигналов, является ТВ-тюнер на основе чипа RTL2832U, в котором обнаружена не де-

кларированная возможность работы в режиме непосредственного доступа к потоку оцифрованных данных. ТВ-тюнер представляет собой компактное устройство, подключаемое к компьютеру с помощью стандартного интерфейса USB 2.0 (рис. 1) [2].



Рис. 1. Внешний вид устройства

В более простом виде работу приемника можно описать в виде:

- 1) антенна, подключенная к тюнеру, принимает сигналы с эфира;
- 2) чип R820T выделяет участок радиодиапазона, начинающийся там, где мы ему указали, и усиливает его;

- 3) чип RTL2832 оцифровывает этот участок и передает по USB на компьютер;

- 4) программа (GnuRadio, SDR# или другая) «настраивается» на выбранную частоту и выполняет демодуляцию указанным способом и отправляет получившийся звук на звуковую карту. Также она может отправлять команды чипу R820T на перестройку на другой участок диапазона [3].

В рамках статьи было проведено исследование канала утечки побочных электромагнитных излучений, с использованием RTL-SDR-приемника.

Исследования интерфейсов VGA и USB показали, что ТВ-тюнер обладает не декларированными возможностями и может быть использован с целью радиомониторинга эфира и обнаружения ПЭМИ. Реализованные функции SDR# позволяют нам производить сканирование частотного диапазона, а также осуществлять поиск выраженного сигнала по заданным критериям. Программный пакет GnuRadio решает задачу по оценке информативности сигнала путем отображения его временной развертки.

Важно отметить что стоимость ТВ-тюнера не превышает 500 рублей. Доступность и простота в использовании позволяет нам применять приемник в учебных целях.

Список литературы

1. Панченко А. А. Мониторинг работы генератора электромагнитного шума с помощью программно-определяемой радиосистемы // Вестн. РГРТУ. 2015. № 53. С. 22–28.
2. Панченко А. А. Оценка возможностей мониторинга радиоэфира с помощью программно-определяемой радиосистемы на основе чипа rtl2832u // Вестн. РГРТУ. 2014. № 50. С. 132–135.
3. URL: <http://xakep.ru/>.

УДК 621.396.621

И. И. Савашинский

Научный руководитель: канд. тех. наук, проф. Д. В. Астрцов
Уральский федеральный университет, Екатеринбург

СКРЫТНОЕ УСТРОЙСТВО РАДИОЭЛЕКТРОННОГО ПОДАВЛЕНИЯ ИЗМЕРИТЕЛЕЙ СКОРОСТИ ДВИЖЕНИЯ ТРАНСПОРТНЫХ СРЕДСТВ И МЕТОДЫ РАДИОЭЛЕКТРОННОЙ ЗАЩИТЫ

Аннотация. Объектами исследования данной работы являются измеритель скорости движения транспортных средств «Искра-1», радар-детектор Escort Passport 9500ix, скрытное устройство для радиоэлектронного подавления измерителей скорости движения транспортных средств. Цель работы состоит в формировании принципов работы скрытного устройства для радиоэлектронного подавления измерителей скорости движения транспортных средств и описании методов радиоэлектронной защиты. В данной работе учитывались ранее опубликованные работы [1–3], связанные с измерителем скорости движения транспортных средств «Искрой-1» — его технические характеристики, принцип действия и конструкция, а также с радар-детектором Escort Passport 9500ix — его возможности и режимы работы. Данная работа является уникальной в своем роде, т. к. скрытное устройство для радиоэлектронного подавления измерителей скорости движения транспортных средств на данный момент находится в стадии разработки и в других работах ранее не рассматривалось. В результате работы сформированы принципы работы скрытного устройства для радиоэлектронного подавления измерителей скорости движения транспортных средств и описаны методы радиоэлектронной защиты.